TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

04998

Expéditeur : L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Destinataire :

voir le formulaire PCT/ISA/220

PCT

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

(règle 43*bis*.1 du PCT)

Date d'expédition *(jour/mois/année)* voir le formulaire PCT/ISA/210 (deuxième feuille)

Référence du dossier du déposant ou du mandataire
voir le formulaire PCT/ISA/220

POUR SUITE À DONNER
Voir le point 2 ci-dessous

Demande internationale No.	Date du dépôt international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR2005/000158	24.01.2005	23.01.2004

Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB
H04L9/32

Déposant
FRANCE TELECOM

1. La présente opinion contient des indications et les pages correspondantes relatives aux points suivants :

- ☒ Cadre n° I Base de l'opinion
- ☐ Cadre n° II Priorité
- ☐ Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- ☐ Cadre n° IV Absence d'unité de l'invention
- ☒ Cadre n° V Déclaration motivée selon la règle 43*bis*.1(a)(i) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- ☐ Cadre n° VI Certains documents cités
- ☐ Cadre n° VII Irrégularités dans la demande internationale
- ☐ Cadre n° VIII Observations relatives à la demande internationale

2. **SUITE À DONNER**

Si une demande d'examen préliminaire internationale est présentée, la présente opinion sera considérée comme une opinion écrite de l'administration chargée de l'examen préliminaire international, sauf dans le cas où le déposant a choisi une administration différente de la présente administration aux fins de l'examen préliminaire international et que l'administration considérée a notifié au Bureau international, selon la règle 66.1bis.b), qu'elle n'entend pas considérer comme les siennes les opinions écrites de la présente administration chargée de la recherche internationale.

Si, comme cela est indiqué ci-dessus, la présente opinion écrite est considérée comme l'opinion écrite de l'administration chargée de l'examen préliminaire international, le déposant est invité à soumettre à l'administration chargée de l'examen préliminaire international une réponse écrite, avec le cas échéant des modifications, avant l'expiration d'un délai de 3 mois à compter de la date d'envoi du formulaire PCT/ISA/220 ou avant l'expiration d'un délai de 22 mois à compter de la date de priorité, le délai expirant le dernier devant être appliqué.

Pour plus de détails sur les possibilités offertes au déposant, se référer au formulaire PCT/ISA/220.

3. Pour de plus amples détails, se référer aux notes relatives au formulaire PCT/ISA/220.

Nom et adresse postale de l'adminstration chargée de la recherche internationale

Office européen des brevets - P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tél. +31 70 340 - 2040 Tx: 31 651 epo nl
Fax: +31 70 340 - 3016

Fonctionnaire autorisé

Holper, G

N° de téléphone +31 70 340-2304

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Demande internationale n° PCT/FR2005/000158

Cadre n° I Base de l'opinion

1. En ce qui concerne la **langue**, la présente opinion a été établie sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous ce point.

   ☐ La présente opinion a été établie sur la base d'une traduction de la langue dans laquelle la demande internationale a été déposée dans la langue suivante , qui est la langue de la traduction remise aux fins de la recherche internationale (selon les règles 12.3 et 23.1.b)).

2. En ce qui concerne **la ou les séquences de nucléotides ou d'acides** aminés divulguées dans la demande internationale, le cas échéant, la recherche internationale a été effectuée sur la base des éléments suivants :

   a. Nature de l'élément :

   ☐ un listage de la ou des séquences

   ☐ un ou des tableaux relatifs au listage de la ou des séquences

   b. Type de support :

   ☐ sur papier sous forme écrite

   ☐ sur support électronique sous forme déchiffrable par ordinateur

   c. Moment du dépôt ou de la remise :

   ☐ contenu(s) dans la demande internationale telle que déposée

   ☐ déposé(s) avec la demande internationale, sous forme déchiffrable par ordinateur

   ☐ remis ultérieurement à la présente administration aux fins de la recherche

3. ☐ De plus, lorsque plus d'une version ou d'une copie d'un listage des séquences ou d'un ou plusieurs tableaux y relatifs a été déposée, les déclarations requises selon lesquelles les informations fournies ultérieurement ou au titre de copies supplémentaires sont identiques à celles initialement fournies et ne vont pas au-delà de la divulgation faite dans la demande internationale telle que déposée initialement, selon le cas, ont été remises.

4. Commentaires complémentaires :

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Demande internationale n° PCT/FR2005/000158

Cadre n° V Déclaration motivée selon la règle 43*bis*.1(a)(i) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-21
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-21
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-21
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE (FEUILLE SEPARÉE)

Demande internationale n° PCT/FR2005/000158

Concernant le point V.

1 Il est fait référence aux documents suivants:
D1 : WO 00/45550 A (FRANCE TELECOM; TELEDIFFUSION DE FRANCE; MATH RIZK; GUILLOU, LOUIS) 3 août 2000 (2000-08-03)

2 Le document D1, qui est considéré comme représentant l'état de la technique le plus pertinent, décrit (voir page 3):
un procédé cryptographique à clés asymétriques selon le préambule de la revendication 1, procédé connu sous l'acronyme GQ2, dans lequel chaque clé publique G_i est de la forme
$G_i = g_i^2 \bmod n$.
dont l'objet de la revendication indépendante 1 diffère en ce que:
chaque clé publique est de la forme $G_i = g_i^A \bmod n$, où $A = 2^{ai}$ et au moins un des a_i est strictement supérieur à 1.

2.1 L'objet de la revendication 1 est donc nouveau (article 33(2) PCT).
Le problème à résoudre par la présente invention peut être considéré comme:
faciliter la recherche de modules RSA compatibles avec le procédé GQ2.

2.2 La solution de ce problème proposée dans la revendication 1 de la présente demande est considérée comme impliquant une activité inventive (article 33(3) PCT), et ce pour les raisons suivantes:

la génération de clés publiques G_i utilisant une mise au carré multiple n'est pas connue ni suggérée dans l'état de la technique.

La revendication 1 remplit donc les critères de nouveauté et d'activité inventive tels que définis dans les articles 33(2) et (3) du PCT.

2.3 Les revendications 2-8 dépendent de la revendication 1 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

3. Les revendications indépendantes 9-21 concernent des réalisations du procédé selon la revendication 1 sous forme de circuit, d'objet portable, de terminal, de système cryptographique, de moyen de stockage, de dispositif de traitement de données ou sous forme de programme ordinateur. Ces revendications satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.